UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,282	06/30/2000	Timothy D. Dodd	05456-105002	9900

7590 01/30/2004

EXAMINER
NORRIS, TREMAYNE M

ART UNIT	PAPER NUMBER
2137	

W Scott Petty
King & Spalding
191 Peachtree Street NE
45th Floor
Atlanta, GA 30303

DATE MAILED: 01/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/608,282	DODD ET AL.	
	Examiner	Art Unit	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,9,10 and 12-16* is/are rejected.

7)☒ Claim(s) *6-8 and 11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4,5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claim 1 rejected under 35 U.S.C. 102(e) as being anticipated by Gleichauf et al.

Regarding claim 1, Gleichauf (US pat 6301668) et al teach a computer-implemented process for identifying security vulnerabilities in a host computer system via a scanner, including the steps of.

passing exploit objects, which contain exploits that check a host computer system for vulnerabilities and resource objects, which contain resources which can be used by the scanner, from an exploit manager and a resource manager to an engine of the scanner; and

executing exploits, which check a host computer system for vulnerabilities, contained in the exploit objects via the engine to identify security vulnerabilities in the host computer system (col.5 lines 15-32; col.5 line 43 thru col.6 line 50; col.7 lines 1-15; col.8 lines 15-18; col.8 line 52 thru col.9 line 3).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2,4,5,9,10,15,16 rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf (US pat 6301668) et al, and further in view of Bowman-Amuah (US pat 6324647).

Regarding claim 2, Gleichauf (US pat 6301668) et al teach a computer-implemented process for identifying security vulnerabilities in a host computer system via a scanner, including the steps of:

installing an express update package containing: an exploit plug-in module containing exploit objects, which contain exploits that check a host computer system for vulnerabilities; a resource plug-in module containing resource objects, which contain resources which can be used by the scanner; a dat file, which contains exploit attribute information (col.6 lines 14-20);

supplying exploit attribute information to an exploit manager from a dat file; passing exploit object and resource object information from the exploit manager and the resource manager to an engine of the scanner; and executing exploits (col.6 lines 5-24). Gleichauf et al, however, do not teach a help file, which contains on-line help information, on a computer. Bowman-Amuah teaches a help file, which contains on-line help information, on a computer (col.9-lines 46-50). It would have been obvious to one of ordinary skill in the art to combine Gleichauf et al's method of vulnerability assessment with Bowman-Amuah's teaching of using an on-line help file in order to aide the user with any questions or concerns regarding usage of the system, which in turn will reduce the leaning curve and help the user to become productive quickly (Bowman-Amuah col.9-lines 46-50).

Regarding claim 4, Gleichauf et al and Bowman-Amuah teach the computer-implemented process of claim 2, in addition Gleichauf et al teach said step of executing exploits includes the steps of

running standard built-in exploits;

running standard plug-in exploits;

running denial of service plug-in exploits; and

running denial of service built-in exploits (col.8 lines 15-18; col.8 lines 52-57).

Regarding claim 5, Gleichauf et al and Bowman-Amuah teach the computer-implemented process of claim 4, in addition Gleichauf et al teach said steps of running standard and denial of service built-in exploits includes the steps of

having the engine get the exploit at the top of a run-order list;

having the engine attempt to run the exploit;

if the exploit is run, recording the exploit result information to a database and a scanner log file (col.5 lines 15-32);

sending the exploit result information to a user interface to display; and

repeating the above steps for the remaining exploits (fig.4; col.5 line 63 thru col.6 line 24; col.8 lines 15-18; col.9 lines 12-18).

Regarding claim 9, Gleichauf et al and Bowman-Amuah teach the computer-implemented process of claim 2, in addition Gleichauf et al teach the step of initializing a scanner (col.5 lines 63-67).

Regarding claim 10, Gleichauf et al and Bowman-Amuah teach the computer-implemented process of 9, in addition Gleichauf et al teach the step of initializing a scanner includes the steps of

enumerating plug-in modules and objects (col.2 lines 19-21);

running load security for each plug-in module (col.7 line 66 thru col.8 line1; col.8 lines 14-18);

initializing a policy manager (col.6 lines 14-24).

Regarding claim 12, Gleichauf et al and Bowman-Amuah teach the computer-implemented process of claim 2, in addition Gleichauf et al teach the step of getting license, policy and host information (col.5 lines 39-48; col.6 lines 24-30).

Regarding claim 15, Gleichauf et al and Bowman-Amuah teach the computer-implemented process of 2, in addition Gleichauf et al teach the steps of:

having host-scanning threads query a session manager for available hosts to scan; having the session manager query the session objects for the next host; and having the session manager return the host to the host-scanning thread (col.7 line 66 thru col.8 line 27; col.9 lines 12-17).

Regarding claim 16, Gleichauf et al and Bowman-Amuah teach the computer-implemented process of claim 2, in addition Gleichauf et al teach the step of running security checks is included (col.5 lines 43-51).

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 3 rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al (US pat 6301668) and Bowman-Amuah (US pat 6324647), and further in view of Howard et al (US pat 6519647).

Regarding claim 3, Gleichauf et al and Bowman-Amuah teach the computer-implemented process of claim 2, however does not teach that said resources can be assigned a namespace based upon the resource's scope. Howard et al teach that said resources can be assigned a namespace based upon the resource's scope (col.3 lines 13-28). It would have been obvious to one of ordinary skill in the art to combine Gleichauf's and Bowman-Amuah's method for vulnerability assessment with Howard et al's teaching of using a namespace associated with a resource in order to have the option of changing the security settings that are associated with individual security settings. (Howard col.3 lines 13-15).

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 13 and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al (US pat 6301688) and Bowman-Amuah (US pat 6324647), and further in view of Gleichauf et al (US pat 6415321).

Regarding claim 13, Gleichauf (US pat 6301668) et al and Bowman-Amuah teach the computer-implemented process of claim 12, but do not teach having the policy manager create a scanpolicy object; having a policy editor examine, modify and configure exploit and resource policy settings; and having the policy editor store the user choices in a policy file. Gleichauf (US pat 6415321) et al teach said step of getting policy information includes the steps of:

having the policy manager create a scanpolicy object (col.5 lines 32-45);

having a policy editor examine, modify and configure exploit and resource policy settings (col.6 lines 47-65); and

having the policy editor store the user choices in a policy file (col.6 lines 31-32). It would have been obvious to combine Gleichauf et al and Bowman-Amuah's method of vulnerability assessment with Gleichauf et al's teaching of a policy manager and policy editor in order to reduce data acquisition overhead and the time needed to obtain network information from network devices (Gleichauf et al US pat 6415321 col.3 lines 10-16).

Regarding claim 14, Gleichauf (US pat 6301668 and US pat 6415321) et al and Bowman-Amuah teach the computer-implemented process of claim 13, in addition

Gleichauf (US pat 6301668) et al teach said step of having a policy manager create the scanpolicy object includes the steps of:

having the policy editor query the policy manager for policy information about an exploit; and

having the policy manager give the policy information to the policy editor (col.8 lines 24-27).

Allowable Subject Matter

Claims 6-8,11 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

With respect to claims 6-8, the cited prior art fails to specifically teach the following steps of running standard and denial of service plug-in exploits that include the steps of:

having the plug-in engine make copies of the master exploit list (a list of exploits and the resources the exploits produce and consume) and the master resource list (a list of resources and the exploits that produce and consume those resources) from the session object;

getting exploit information from the scanpolicy object for the first exploit;

creating a target object and putting the exploit information in the target object;

passing the target object to the exploit object;

running the exploit;

adding exploit result information to the target object;

passing the target object back to a plug-in engine;

querying the target object for exploit result information;

recording exploit result information to the scanner log file and sending the exploit result information to the user interface; and

repeating the above steps for the remaining exploits.

With respect to claim 11 the cited prior art fails to specifically teach the following steps of:

asking an exploit manager and a resource manager to identify available exploits and resources;

having the exploit manager and the resource manager query the registry for available exploit objects and the available resource objects;

having the exploit manager and the resource manager create maps indicating which plug-in modules contain the available exploit objects and the available resource objects;

having a policy manager ask the exploit manager and resource manager for the available exploit objects and common-setting resource objects;

creating the available exploit objects and common-setting resource objects;

having the policy manager query the available exploit objects and common setting resource objects.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Tremayne Norris

January 21, 2004

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137